UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JOSEPH T. SCHESSO, Defendant.	CASE NO. CR11-5285 RJB MEMORANDUM OPINION RE MOTION TO SUPPRESS EVIDENCE

This matter comes before the Court on Defendant Joseph T. Schesso's Motion to Suppress Evidence seized from his home pursuant to a search warrant issued and executed on June 30, 2010. Dkt. 64. The Court has considered the motion, the government's response (Dkt. 74), reply (Dkt. 78), the warrant (Dkt. 64-1 pp. 36-39), the application for warrant (Dkt. 64-1 pp. 4-35), and the representations and arguments of counsel at a hearing conducted October 21, 2011.

At the conclusion of the hearing, the Court entered an oral ruling granting the motion to suppress. Dkt. 79. The transcript of the Court's oral ruling (Dkt. 88) is attached as Exhibit 1, and is incorporated herein by this reference. The Court also entered an Order Granting Motion

to Suppress Evidence. Dkt. 82. This memorandum opinion formalizes and supplements the oral ruling.

INTRODUCTION AND BACKGROUND

The Warrant Application

Due to perceived constraints placed on federal search warrants of computers, Immigration and Customs Enforcement (ICE) agents requested assistance from state law enforcement personnel in obtaining and executing the search warrant. Dkt. 74 pp. 5. In collaboration with ICE, on June 3, 2010, an officer of the Vancouver Police Department sought permission in the District Court of Clark County, Washington, to search and seize evidence of two crimes: Dealing in depictions of a minor engaged in sexually explicit conduct (RCW 9.68A.050) and Possession of depictions of a minor engaged in sexually explicit conduct (RCW 9.68A.070). Dkt. 64-1 pp. 8, 30. The application for the warrant did not contain any of the protocols for a search of electronically stored information suggested by the concurring opinion in *United States v. Comprehensive Drug Testing, Inc.,* 621 F.3d 1162 (9th Cir. 2010) (*CDT III*), nor did it address the need for "greater vigilance" required by *CDT III*.

The search warrant application states that in December of 2008, German law enforcement personnel informed ICE that an investigation of a child pornography peer-to-peer file sharing network known as “eDonkey” had revealed that illicit images were distributed to and by computers in the United States. The German investigation revealed that during a four hour period on October 20, 2008, a computer with an IP address of 97.115.106.34 was making available for download, copies of a file containing child pornography. Dkt. 64-1 pp. 17-18. The German authorities confirmed that the hash value (digital foot print) of the file offered by the computer at IP address 97.115.106.34 matched the hash value of a known file containing child

pornography. *Id.* The eDonkey hash value of the file matched the hash value of a child pornography video in German authority's contraband files library. *Id.* The German authorities supplied ICE agents a copy of the file. *Id.,* at pp. 18. ICE investigators determined that the IP address was assigned to Defendant Schesso at his Vancouver, Washington residence. *Id*., at pp. 20-21. Based on this single four hour incident in October 2008, the Vancouver Police Department, in collaboration with ICE, filed the June 2010 application for search warrant.

The application seeks broad authorization to seize and examine every sort of computer storage device and records found at Schesso's residence. Dkt. 64-1 pp. 23-28. The application also seeks unlimited authorization to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. *Id*., at 28-30

The remainder of the application consists of a set of "definitions" related to cybercrime investigations (Dkt. 64-1 pp. 8-10); a general explanation of how computers and the Internet operate (*Id*., at 10-14, 16); and a generic pornography "collector profile" (*Id*. at 14-16). There is nothing in the application that directly connects this generic information regarding child pornographers to the Defendant. There is no information in the application that the named storage devices are the type typically used in connection with computer peer-to peer file sharing as found in the investigation of Defendant Schesso.

The Search Warrant

The search warrant did not name the particular crimes that the investigators were aware of, but found probable cause to search for evidence of the crimes of Revised Code of Washington ("RCW") 9.68A.050 Dealing In Depictions Of A Minor Engaged In Sexually Explicit Conduct, and RCW 9.68A.070 Possession Of Depictions Of A Minor Engaged In Sexually Explicit Conduct. Dkt. 64-1 pp. 36. The warrant provided for the search and seizure of

any computer or electronic equipment or digital data storage devices that are capable of being used to commit or further the crimes, or to create, access, or store the types of evidence, contraband, fruits, or instrumentalities of such crimes. *Id.*, at 36-39. Upon execution of the warrant at the Defendant's home, officers seized computers and all electronic media capable of storing, transporting, and viewing electronic data. Dkt. 74-1 pp. 12.

Forensic examination of a seized 16MB Fujifilm camera media card revealed six deleted but recoverable pictures of a young, prepubescent girl's genital area. Dkt. 74-1 pp. 8. Data embedded in the six pictures confirms that they were taken with a Fujifilm FinePix S5100 camera, the same make and model of camera physically connected to Schesso's computer and seized at his residence. *Id.*, at pp. 9. Subsequent investigation revealed that the prepubescent girl depicted was Schesso's niece. Dkt. 74 pp. 8. Along with the six images of Schesso's niece, forensic examination of Schesso's electronic media revealed over 3,400 images of commercial child pornography and approximately 632 videos of child pornography, including the video shared over the eDonkey peer-to-peer network. Dkt. 74-1 pp. 8.

Federal Prosecution

Based upon the discovery of the evidence of child pornography, the U.S. Attorney's office was contacted regarding federal prosecution. Dkt. 74-1 pp. 10. A four count federal indictment was filed against Schesso. Dkt. 25. Count I charged Schesso with Production of Child Pornography/Sexual Exploitation of Children, 18 U.S.C. §§ 2251(a) and 2251(e). Count 2 charged Schesso with Distribution of Material Constituting or Containing Child Pornography, 18 U.S.C. §§ 2252A(a)(2) and 2252A(b)(1). Count 3 charged Schesso with Receipt of Material Constituting or Containing Child Pornography, 18 U.S.C. §§ 2252A(a)(2) and 2252A(b)(1).

Count 4 charged Schesso with Possession of Child Pornography, 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(b)(2). Dkt. 25 pp. 1-4.

The motion to suppress evidence of the search followed. Defendant contends that the warrant was overbroad and contained none of the safeguards for electronic data searches required by the Fourth Amendment.

FOURTH AMENDMENT AND ELECTRONIC DATA SEARCHES

The primary issue before the Court is whether the search warrant is facially overbroad based on the showing in the affidavit for the warrant.

The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

A warrant must be specific to prevent law enforcement officers from conducting general, exploratory searches at their discretion. *United States v. Adjani*, 452 F.3d 1140, 1147 (9th Cir. 2006). The level of specificity required is not a precise formula but rather depends on the particular circumstances and the type of evidence sought. *United States v. Hill*, 459 F.3d 966, 973 (9th Cir.2006). A warrant describing a category of items is not invalid if a more specific description is impossible. *Id.* Specificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based. *Id.*, at 973. When reviewing challenges to a warrant's specificity, courts consider one or more of the following factors: (1) whether probable cause exists to seize all items of a particular type described in the warrant; (2) whether the warrant sets out objective standards

by which executing officers can differentiate items subject to seizure from those which are not; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued. *Adjani*, at 1148.

Review of this search warrant is further guided by *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982) and *U.S. v. Comprehensive Drug Testing, Inc.,* 621 F.3d 1162 (9th 2010)(*CDT III*). In *CDT III* the Court stated that "[t]he point of the *Tamura* procedures is to maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search of office file systems and computer databases. If the government can't be sure whether data may be concealed, compressed, erased or booby-trapped without carefully examining the contents of every file—and we have no cavil with this general proposition—then everything the government chooses to seize will, under this theory, automatically come into plain view." *CDT III*, at 1170-71. "This would make a mockery of *Tamura* and render the carefully crafted safeguards in the Central District warrant a nullity." *Id*., at 1171. In concluding remarks the Court in *CDT III* stated:

> This pressing need of law enforcement for broad authorization to examine electronic records, …. creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant. The problem can be stated very simply: There is no way to be sure exactly what an electronic file contains without somehow examining its contents — either by opening it and looking, using specialized forensic software, keyword searching or some other such technique. But electronic files are generally found on media that also contain thousands or millions of other files among which the sought-after data may be stored or concealed. By necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there.
>
> Once a file is examined, however, the government may claim …. that its contents are in plain view and, if incriminating, the government can keep it. Authorization to search some computer files therefore automatically becomes authorization to search all files in the same sub-directory, and all files in an enveloping directory, a neighboring hard drive, a nearby computer or nearby storage media….
>
> ….

> Everyone's interests are best served if there are clear rules to follow that strike a fair balance between the legitimate needs of law enforcement and the right of individuals and enterprises to the privacy that is at the heart of the Fourth Amendment. *Tamura* has provided a workable framework for almost three decades, and might well have sufficed in this case had its teachings been followed. We have updated *Tamura* to apply to the daunting realities of electronic searches.
>
> We recognize the reality that over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records. This calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect.

CDT, at1177. See also Dkt. 88 pp. 53-54.

With these principles in mind, a review of the application for the search warrant demonstrates that it did not support probable cause for the issuance of a general warrant for the search and seizure of any electronic storage devices for evidence of child pornography crimes. The generalized statements regarding cybercrime and pornography collector profiles do not demonstrate that Schesso had some proclivity or likelihood of committing crimes other than the particular crime(s) described in the single incident of file sharing that occurred on October 20, 2008, particularly when the warrant was not sought for some 20 months after the date of the alleged crimes. The application for the search warrant does not support a warrant for the search and seizure of any and all electronic storage devices found at Schesso's residence in order to comb through these devices to determine what other crimes may have been committed.[1] The

---

[1] If the warrant had been limited, only authorizing a search for evidence of the crimes known to the investigators, it is possible that, in exercising the warrant, they would have come across evidence of other crimes or evidence, which may have then been usable in further proceedings.

application did not justify a generalized search in this case. The affidavit simply does not support the warrant. The warrant is facially deficient. To rule to the contrary would be to say that if any person ever had a child pornography file or made such a file available to download on a peer-to-peer network, that person is subject to a general search of all of that person's computer-related equipment without reference to the particular crime or crimes that are known to law enforcement. That is not a reasonable search under the Fourth Amendment, as that amendment has been interpreted and applied by the courts, and in particular interpreted and applied most recently by the Ninth Circuit in *CDT III*. See also Dkt. 88 pp. 54-59

The constitution forecloses unlimited computer searches based on this type of seize-it-all-and-sort-it-out-later warrant that was obtained in this case. This was a general warrant, not justified or supported by the affidavit, and was facially deficient.

EXCLUSION OF EVIDENCE

The government asserts that application of the "good faith" exception to the exclusion rule avoids the necessity of exclusion of the evidence. See *United States v. Leon*, 468 U.S. 897 (1984). In *Leon,* the Supreme Court held that evidence seized by police officers acting in good faith pursuant to a facially valid warrant would be admissible even though the warrant was subsequently found to lack probable cause. The Court cautioned, however, that "[i]n so limiting the suppression remedy, we leave untouched the probable-cause standard and the various requirements for a valid warrant." *Id.*, at 923. The Court expressly refused to apply the good-faith exception to warrants which fail to adequately specify the place to be searched or the items to be seized. *Id.* Furthermore, the Court noted that its holding was based on an assumption "that the officers properly executed the warrant and searched only those places and for those objects that it was reasonable to believe were covered by the warrant." *Id.*, at 918 n. 19. This language

indicates that application of the *Leon* exception to the exclusionary rule should not apply to facially overbroad warrants or to searches which exceed the scope of the warrant.

The good faith exception is inapplicable in the context of this action where the overbroad warrant is so facially deficient that reliance on it is not reasonable. See *U.S. v. Kow,* 58 F.3d 423, 428-29 (9th Cir. 1995); *U.S. v. Spilotro*, 800 F.2d 959, 968 (9th Cir. 1986); *United States v. Washington*, 782 F.2d 807, 819 (9th Cir.1986); *U.S. v. Crozier*, 777 F.2d 1376, 1381-82 (9th Cir. 1985). This is particularly true where the agents knowingly opted to seek a forum that might accept a less particular and specific warrant than a federal magistrate would require (*see* Dkt. 74 at 5).

The warrant in this case is so broad and deviates so far from well-established Fourth Amendment standards that the searches based on that warrant cannot be defended on the basis of good faith. Exclusion of the evidence is appropriate.

CONCLUSION

For the reasons stated orally on the record by the Court and as addressed in this memorandum opinion, the suppression of evidence seized from Defendant's home pursuant to a search warrant issued on June 30, 2010, and all fruits of such evidence, and items seized pursuant to a second warrant stemming from the June 30, 2010, search, is required by the Fourth Amendment to the United States Constitution.

Dated this 9th day of November, 2011.

ROBERT J. BRYAN
United States District Judge